We claim:

1. A method for transforming a message represented as an element of a complete residue set modulo a prime number p into a Montgomery residue of a multiplicative inverse, the method comprising:

selecting a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize, and m is greater than a bit-length of the prime number p;

determining (r, k) from an almost Montgomery inverse function;

if k is less than m, then assigning r a value obtained as a Montgomery product of r and R^2 mod p, and assigning k a value $k = k + m$; and

obtaining the multiplicative inverse as a Montgomery product of r and 2^{2m-k}.

2. The method of claim 1, further comprising retrieving a stored value of R^2 mod p.

3. A computer-readable medium containing instructions for performing the method of claim 2.

4. A computer-readable medium containing instructions for performing the method of claim 1.

5. A cryptographic system for encryption and decryption, the system comprising a module for transforming a message as recited in claim 1.

6. The method of claim 1, wherein the message is a ciphertext.

7. A method for obtaining a classical inverse of a message, represented as a series of binary digits, that is an element of a residue set modulo a prime number p, the method comprising:

obtaining values (r,k) by calculating an almost Montgomery inverse function of the representation of the message using a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize and is greater than a bit-length of the prime number p;

if k is greater than m, then assigning r a value equal to a Montgomery product of r and 1, and assigning k a value of $k - m$; and

calculating the classical inverse as a Montgomery product of r and 2^{m-k}.

8. A cryptographic system, comprising an encryption/decryption module that performs the method of claim 7.

9. The cryptographic system of claim 8, further comprising at least one integrated circuit.

10. A computer-readable medium, comprising instructions for performing the method of claim 7.

11. A cryptographic method, comprising:

representing a message as a series of binary digits, the series being divisible into an integer number m of words;

selecting a prime number p;

obtaining an intermediate product r and an integer k using an almost Montgomery inverse procedure, wherein a Montgomery radix $R = 2^m$, and m is greater than a bit-length of the prime number p;

if $k < m$, then assigning r a value obtained as a Montgomery product of r and R^2 mod p, and assigning k a value of $k + m$;

assigning r a value obtained as a Montgomery product of r' and R^2 mod p; and

a1

obtaining a multiplicative inverse as a Montgomery product of r and 2^{2m-k}.

12. The method of claim 11, further comprising retrieving a stored value of R^2 mod p.

13. A computer-readable medium containing instructions for performing the method of claim 12.

14. A method for computing a classical inverse of a message a, the method comprising:

(a) selecting an integer m that is greater than a bit-length of the message a, and selecting a Montgomery radix $R = 2^m$;

(b) selecting a prime number p;

(c) representing the message a as a series of binary digits, the series being divided into m words;

(d) obtaining a value $r = a^{-1}2^m \pmod{p}$;

(e) obtaining the classical inverse as a Montgomery product of r and 1.

15. A method for computing a classical inverse of a message a, the method comprising:

(a) selecting an integer m that is greater than a bit-length of the message a, and selecting a Montgomery radix $R = 2^m$;

(b) selecting a prime number p;

(c) representing the message a as a series of binary digits, the series being divided into m words;

(d) obtaining a value r as a Montgomery product of the message a and R^2 mod p; and

(e) obtaining the classical inverse as a Kaliski inverse of r.

16. A method for computing a multiplicative inverse of an M-residue $A = a2^m \bmod p$, wherein p is a prime number, m is an integer, and a Montgomery radix $R = 2^m$, the method comprising: computing an intermediate product r and an integer k using an almost Montgomery inverse procedure;

assigning an intermediate product r' the value of a Montgomery product of r and R^2; and

obtaining the multiplicative inverse as a Montgomery product of r' and 2^{2m-k}.

17. The method of claim 16, further comprising:

determining if the integer k is greater than or equal to m; and

if the integer k is k is greater than or equal to m, assigning the intermediate product r' the value of a Montgomery product of r and R^2 and assigning k a value of $k + m$ prior to obtaining the step of obtaining the multiplicative inverse.

18. The method of claim 16, further comprising retrieving a value of R^2 mod p.

19. A computer-readable medium containing instructions for performing the method of claim 18.

20. A cryptographic method for processing a series of binary digits divided into an integer number m of words, the method comprising:

selecting a Montgomery radix $R = 2^m$ and a prime number p;

executing an almost Montgomery inverse procedure to obtain an intermediate value r and an integer k; and

obtaining a Montgomery product of r.

21. A cryptographic method, comprising:

dividing a message into at least two words;

selecting a Montgomery radix based on a number of words in the message; and

performing a Montgomery multiplication to transform the message.